What Is Claimed Is:

1.   1.   A method for detecting a failure sequence or other undesirable
2   system behavior in a computer system and subsequently taking a corresponding
3   remedial action, comprising:
4   receiving instrumentation signals from the computer system while the
5   computer system is operating;
6   determining from the instrumentation signals if the computer system is in
7   a failure sequence that is likely to lead to undesirable system behavior, such as a
8   system crash;
9   wherein the determination involves considering predetermined
10   multivariate correlations between multiple instrumentation signals and a failure
11   sequence that is likely to lead to undesirable system behavior; and
12   if the computer system is in a failure sequence that is likely to lead to
13   undesirable system behavior, taking a remedial action.

1.   2.   The method of claim 1, wherein taking the remedial action
2   involves generating an alarm.

1.   3.   The method of claim 2, wherein generating the alarm involves
2   communicating the alarm to a system administrator so that the system
3   administrator can take the remedial action.

1.   4.   The method of claim 3, wherein communicating the alarm to the
2   system administrator involves communicating information specifying the nature
3   of the failure sequence to the system administrator.

14

1   5.   The method of claim 1, wherein taking the remedial action can

2 involve: killing processes, blocking creation of new processes, or throwing away

3 work, until the system is no longer in a failure sequence that is likely to lead to

4 undesirable system behavior.

1   6.   The method of claim 1, wherein determining if the computer

2 system is in a failure sequence involves:

3   deriving estimated signals for a number of instrumentation signals,

4 wherein each estimated signal is derived from correlations with other

5 instrumentation signals; and

6   comparing an actual signal with an estimated signal for a number of

7 instrumentation signal to determine whether the computer system is in a failure

8 sequence.

1   7.   The method of claim 6, wherein comparing an actual signal with an

2 estimated signal involves using sequential detection methods to detect changes in

3 a relationship between the actual signal and the estimated signal.

1   8.   The method of claim 7, wherein the sequential detection methods

2 include the Sequential Probability Ratio Test (SPRT).

1   9.   The method of claim 6, wherein prior to deriving the estimated

2 signal, the method further comprises determining correlations between

3 instrumentation signals in the computer system, whereby the correlations can

4 subsequently be used to generate estimated signals.

15

1   10.   The method of claim 9, wherein determining the correlations

2   involves:

3   deliberately overloading the computer system during a test mode to

4   produce undesirable system behavior, such as a system crash; and

5   identifying multivariate correlations between multiple instrumentation

6   signals and the system crash.

1   11.   The method of claim 9, wherein determining the correlations

2   involves using a non-linear, non-parametric regression technique to determine the

3   correlations.

1   12.   The method of claim 11, wherein the non-linear, non-parametric

2   regression technique can include a multivariate state estimation technique.

1   13.   The method of claim 1, wherein the instrumentation signals can

2   include:

3   signals associated with internal performance parameters maintained by

4   software within the computer system;

5   signals associated with physical performance parameters measured

6   through sensors the computer system; and

7   signals associated with canary performance parameters for synthetic user

8   transactions, which are periodically generated for performance measuring

9   purposes.

1   14.   A computer-readable storage medium storing instructions that

2   when executed by a computer cause the computer to perform a method for

3   detecting a failure sequence or other undesirable system behavior in a computer

16

4   system and subsequently taking a corresponding remedial action, the method

5   comprising:

6   receiving instrumentation signals from the computer system while the

7   computer system is operating;

8   determining from the instrumentation signals if the computer system is in

9   a failure sequence that is likely to lead to undesirable system behavior, such as a

10   system crash;

11   wherein the determination involves considering predetermined

12   multivariate correlations between multiple instrumentation signals and a failure

13   sequence that is likely to lead to undesirable system behavior; and

14   if the computer system is in a failure sequence that is likely to lead to

15   undesirable system behavior, taking a remedial action.

1   15.   The computer-readable storage medium of claim 14, wherein

2   taking the remedial action involves generating an alarm.

1   16.   The computer-readable storage medium of claim 15, wherein

2   generating the alarm involves communicating the alarm to a system administrator

3   so that the system administrator can take the remedial action.

1   17.   The computer-readable storage medium of claim 16, wherein

2   communicating the alarm to the system administrator involves communicating

3   information specifying the nature of the failure sequence to the system

4   administrator.

1   18.   The computer-readable storage medium of claim 16, wherein

2   taking the remedial action can involve: killing processes, blocking creation of new

17

3   processes, or throwing away work, until the system is no longer in a failure

4   sequence that is likely to lead to undesirable system behavior.

1   19.   The computer-readable storage medium of claim 14, wherein

2   determining if the computer system is in a failure sequence involves:

3   deriving estimated signals for a number of instrumentation signals,

4   wherein each estimated signal is derived from correlations with other

5   instrumentation signals; and

6   comparing an actual signal with an estimated signal for a number of

7   instrumentation signal to determine whether the computer system is in a failure

8   sequence.

1   20.   The computer-readable storage medium of claim 19, wherein

2   comparing an actual signal with an estimated signal involves using sequential

3   detection methods to detect changes in a relationship between the actual signal

4   and the estimated signal.

1   21.   The computer-readable storage medium of claim 20, wherein the

2   sequential detection methods include the Sequential Probability Ratio Test

3   (SPRT).

1   22.   The computer-readable storage medium of claim 19, wherein prior

2   to deriving the estimated signal, the method further comprises determining

3   correlations between instrumentation signals in the computer system, whereby the

4   correlations can subsequently be used to generate estimated signals.

18

1 23. The computer-readable storage medium of claim 22, wherein
2 determining the correlations involves:
3   deliberately overloading the computer system during a test mode to
4 produce undesirable system behavior, such as a system crash; and
5   identifying multivariate correlations between multiple instrumentation
6 signals and the system crash.

1 24. The computer-readable storage medium of claim 22, wherein
2 determining the correlations involves using a non-linear, non-parametric
3 regression technique to determine the correlations.

1 25. The computer-readable storage medium of claim 24, wherein the
2 non-linear, non-parametric regression technique can include a multivariate state
3 estimation technique.

1 26. The computer-readable storage medium of claim 14, wherein the
2 instrumentation signals can include:
3   signals associated with internal performance parameters maintained by
4 software within the computer system;
5   signals associated with physical performance parameters measured
6 through sensors the computer system; and
7   signals associated with canary performance parameters for synthetic user
8 transactions, which are periodically generated for performance measuring
9 purposes.

19

1   28.   An apparatus that detects a failure sequence or other undesirable

2   system behavior in a computer system and subsequently takes a corresponding

3   remedial action, comprising:

4   a monitoring mechanism configured to monitor instrumentation signals

5   from the computer system while the computer system is operating;

6   a determination mechanism configured to determine from the

7   instrumentation signals if the computer system is in a failure sequence that is

8   likely to lead to undesirable system behavior, such as a system crash;

9   wherein the determination mechanism is based on multivariate

10   correlations between multiple instrumentation signals and a failure sequence that

11   is likely to lead to undesirable system behavior; and

12   a remediation mechanism that is configured to take a remedial action if the

13   computer system is in a failure sequence that is likely to lead to undesirable

14   system behavior.

15

20